Cyber Security for Education

Protecting and Securing your Data in Office 365

Cyber Security for Education

Edwin Guarin, Solution Specialist
Steve Faehl, Cloud Architect
Department of Defense makes Office 365 available for purchase

Where is my data?

These interactive data maps provide specific geographic details about where customer data is stored in Microsoft Office 365 and Microsoft Dynamics 365. Specifically, they provide information regarding the locations of our datacenters throughout the world for the Office 365 and Dynamics 365 services.

Location of customer data at rest

Quincy, WA
Chicago, IL

Azure Active Directory
Office 365
- Exchange Online
- SharePoint Online
- Skype for Business
- Project Online

San Antonio, TX

Azure Active Directory
Office 365
- Exchange Online
- SharePoint Online
- Skype for Business
- Project Online

Microsoft Dynamics Marketing

Boydton, VA

Azure Active Directory
Office 365
- Exchange Online
- Yammer

This data map describes where Microsoft stores customer data in the course of providing Office 365 and Dynamics 365 services for customers located in North America. Specifically, this map provides information regarding the locations of all datacenters and corresponding services for customer data stored in Office 365 and Dynamics 365 services in North America.

Microsoft replicates customer data in at least two datacenters at any given time for reliability and availability.
Cyber Security is the #1 concern of organizations and governments.
A layered security approach is necessary to safeguard productivity.
Service-level security capabilities
Defense in depth

- Physical controls, video surveillance, access control
- Edge routers, firewalls, intrusion detection, vulnerability scanning
- Access control and monitoring, anti-malware, patch and configuration management
- Secure engineering (SDL), access control and monitoring, anti-malware
- Account management, training and awareness, screening
- Threat and vulnerability management, security monitoring, and response, access control and monitoring, file/data integrity, encryption

Independently verified to meet key standards – ISO 27001, 27018, SSAE 16 (SOC 1 & 2) Type II, FISMA
Physical Security

- Perimeter security
- Fire Suppression
- Multi-factor authentication
- Extensive monitoring

Seismic bracing
24x7 onsite security staff
Days of backup power
Tens of thousands of servers
Host/Application

- Patching/Malware protection
- Whitelisted processes
- Security Development Lifecycle
- Automated tooling for routine activities
- Zero standing permissions in the service
- Auditing of all operator access and actions
Administrators

Personnel
Background checks
Screening

Account Management
Automatic account deletion
Unique accounts
Zero access privileges

Training, policies and awareness
SDL
Annual training
Just-in-time access

Engineers must have current background check, fingerprinting, security training.

System grants least privilege required to complete task.
Customer data isolation

Designed to support logical isolation of data that multiple customers store in same physical hardware.

Intended or unintended mingling of data belonging to a different customer/tenant is prevented by design using Active Directory organizational units.
Encryption

Data in transit
- Strong SSL/TLS cipher suite
- Perfect Forward Secrecy
- Datacenter-to-datacenter encryption

Data at rest
- BitLocker disk encryption
- Per-file encryption for customer content
Encryption at rest with Per-file Encryption
Assume Breach

- Monitor emerging threats
- Execute post breach
- War-game exercises
- Red teaming
- Insider attack simulation
- Blue teaming
Customer security controls
Protecting your data at various vectors
Simplify and Protect: Securing Identity with Azure Active Directory

Enabling users and organizations with a common identity on-premises and in the cloud

- Multi-Factor Authentication for additional user identity verification
- Single Sign On with Federation
Multi-factor authentication using any phone

**Mobile Apps**
- Push Notification
  - One-Time-Passcode (OTP) Token

**Phone Calls**
- Out-of-Band* Call

**Text Messages**
- Text
  - One-Time Passcode (OTP) by Text

*Out of band refers to being able to use a second factor with no modification to the existing app UX.
Mobile Device Management

- Conditional Access
- Device Management
- Selective Wipe
- Advanced Application Management

Built-in + Microsoft Intune
Encryption technologies

Azure Rights Management Service

S/MIME

Office 365 Message Encryption

Transport Layer Security
Data Loss Prevention

- Identify
- Monitor
- Protect
- End user education

Helps to identify, monitor, protect sensitive data through deep content analysis.
DLP document fingerprinting

Scan email and attachments to look for patterns that match document templates

Protect sensitive documents from being accidently shared outside your organization

No coding required; simply upload sample documents to create fingerprints

---

<table>
<thead>
<tr>
<th>Name</th>
<th>Standard Bank Forms</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRS Tax Forms</td>
<td></td>
</tr>
</tbody>
</table>

You can use document fingerprints to customize sensitive information types in your policies.

### Standard Bank Forms

This sensitive information type will detect any of the standard bank forms, like a loan application, account information, etc.

- Account opening form - Business.pdf
- Account opening form - Personal.pdf
- Account opening form - Priority.pdf
- Auto loan application for business.pdf
- Auto loan application for salaried individual.pdf
- Cash Deposit Slip.pdf
- Cheque Deposit Slip.pdf
- Credit Card application form.pdf

1 selected of 2 total
## Email archiving and retention

<table>
<thead>
<tr>
<th>Preserve</th>
<th>Search</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>In-Place Archive</strong></td>
<td><strong>eDiscovery</strong></td>
</tr>
<tr>
<td>Secondary mailbox with separate quota</td>
<td>Web-based eDiscovery Center and multi-mailbox search</td>
</tr>
<tr>
<td>Managed through EAC or PowerShell</td>
<td>Search primary, In-Place Archive, and recoverable items</td>
</tr>
<tr>
<td>Available on-premises, online, or through EOA</td>
<td>Delegate through roles-based administration</td>
</tr>
</tbody>
</table>

### Governance
- Automated and time-based criteria
- Set policies at item or folder level
- Expiration date shown in email message

### Hold
- Capture deleted and edited email messages
- Time-Based In-Place Hold
- Granular Query-Based In-Place Hold
- Optional notification

### eDiscovery
- Auditing to ensure controls are met
Anti Spam/ Anti Virus

• Multi-engine antimalware protects against 100% of known viruses
• Continuously updated anti-spam protection captures 98%+ of all inbound spam
• Advanced fingerprinting technologies that identify and stop new spam and phishing vectors in real time
• Mark all bulk messages as spam
• Block unwanted email based on language or geographic origin
Next-Gen Protection Benchmarks

- Leverage big data and machine learning
- Analyze signature and behavior for zero-day protection
- Deep insights driving rapid iterative innovation
- Actionable reporting that cuts through the noise
- People-centric protection
Advanced Threat Protection

Safe Links and Safe Attachments

Phishing Visibility

Blocked URL
Cloud App Security

General dashboard

- 2.7K activities monitored
- 401 files monitored
- 2.9K users monitored
- 0 governance actions taken
- 0 user notifications sent

- Access file https://brunetti-my.sharepoint.com/User...
  - test1: Microsoft OneDrive
  - 207.46.137.24
  - Hong Kong SAR
  - May 19, 2016, 1:37 AM
- Failed log on test1@edudemo.us (The entered and s...
  - test1: Office 365
  - 137.135.107.246
  - United States
  - May 5, 2016, 8:44 AM
- Failed log on test1@edudemo.us (The entered and s...
  - test1: Office 305
  - 137.135.91.93
  - United States
  - Apr 27, 2016, 10:46 AM

- Logon from a risky IP address
  - test1@edudemo.us
  - Microsoft OneDrive
  - 6 minutes ago
- New location
  - test1@edudemo.us
  - Microsoft OneDrive
  - 41 minutes ago
- General anomaly detection
  - an hour ago

Top 3 alert types
- Activity policy alert: 4
- Suspicious activity alert: 4
Compliance

What does compliance mean to customers?
What standards do we meet?
What is regulatory compliance and organizational compliance?
Compliance
Commitment to industry standards and organizational compliance

Service-level capabilities for global compliance
- Enable customers to meet global compliance standards in ISO 27001, 27018, EUMC, HIPAA, FedRAMP/FISMA.
- Contractually commit to privacy, security and handling of customer data through Data Processing Agreements

Customer controls for compliance with internal policies
- Admin Controls like Data Loss Prevention, Archiving, E-Discovery to enable organizational compliance
## Standards & Certifications

<table>
<thead>
<tr>
<th>Standards Certifications</th>
<th>Market</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSAE/SOC</td>
<td>Finance</td>
<td>Global</td>
</tr>
<tr>
<td>ISO 27001:2013</td>
<td>Global</td>
<td>Global</td>
</tr>
<tr>
<td>ISO 27018</td>
<td>Global</td>
<td>Global</td>
</tr>
<tr>
<td>EUMC</td>
<td>Europe</td>
<td>Europe</td>
</tr>
<tr>
<td>FERPA</td>
<td>Education</td>
<td>U.S.</td>
</tr>
<tr>
<td>FedRAMP/FISMA</td>
<td>Government</td>
<td>U.S.</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Healthcare</td>
<td>U.S.</td>
</tr>
<tr>
<td>HITECH</td>
<td>Healthcare</td>
<td>U.S.</td>
</tr>
<tr>
<td>ITAR</td>
<td>Defense</td>
<td>U.S.</td>
</tr>
<tr>
<td>HMG IL2</td>
<td>Government</td>
<td>UK</td>
</tr>
<tr>
<td>CJIS</td>
<td>Law Enforcement</td>
<td>U.S.</td>
</tr>
<tr>
<td>Article 29 +</td>
<td>Europe</td>
<td>Europe</td>
</tr>
<tr>
<td>SOC 2</td>
<td>Global</td>
<td>Global</td>
</tr>
</tbody>
</table>

*EU Data Protection Authorities validate Microsoft’s approach to privacy*
How does Office 365 meet Compliance...

<table>
<thead>
<tr>
<th>Office 365 Service</th>
<th>Master GRC Control Sets</th>
<th>Certifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Capabilities</strong></td>
<td><strong>Office 365 has over 1000 controls Today!</strong></td>
<td></td>
</tr>
<tr>
<td>Physical Security</td>
<td>Access Control</td>
<td>ISO</td>
</tr>
<tr>
<td>Security Best Practices</td>
<td>Data Minimization &amp; Retention</td>
<td>FedRAMP</td>
</tr>
<tr>
<td>Secure Network Layer</td>
<td>Account Mgmt.</td>
<td>SSAE 16</td>
</tr>
<tr>
<td>Data Encryption</td>
<td>Incident Monitoring</td>
<td>HIPAA</td>
</tr>
<tr>
<td><strong>Customer Controls</strong></td>
<td>Data Encryption</td>
<td>New Cert’s and more...</td>
</tr>
<tr>
<td>DLP</td>
<td>Encryption of stored data and more...</td>
<td></td>
</tr>
<tr>
<td>OME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMIME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RBAC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Office 365
Privacy by design means that we do not use your information for anything other than providing you services.

**No Advertising**
- No advertising products out of Customer Data
- No scanning of email or documents to build analytics or mine data

**Transparency**
- Access to information about geographical location of data, who has access and when
- Notification to customers about changes in security, privacy and audit information

**Privacy controls**
- Various customer controls at admin and user level to enable or regulate sharing
- If the customer decides to leave the service, they get to take to take their data and delete it in the service
Backed up by contractual commitments

- Privacy terms
- Security terms
- EU Model Clauses
- Response to government demands
- Core service features and simpler, stable terms during a subscription

Standard Online Service Terms apply to every cloud customer—no amendments or negotiations required.
Microsoft is demonstrating our commitment to protect customer data from government demands in court actions.

**U.S. Warrant Case.** Microsoft is in litigation with the U.S. government to resist a criminal search warrant seeking customer data stored outside the United States. The case is on appeal. It raises important questions about the ability of the U.S. government to issue search warrants for data outside the U.S., given that the government clearly cannot search homes or business premises abroad.

**National Security Letters.** Microsoft resisted a National Security Letter non-disclosure order, which prohibited Microsoft from notifying the customer of a government demand to disclose its data. The FBI withdrew the demand.

**Government Requests Transparency.** Microsoft filed a lawsuit against the U.S. government to permit greater disclosure about government demands for customer data. The U.S. government settled, allowing Microsoft and others to share broader information with customers.